Service Description

Point to Point Encryption Solution Assessment

Contents

P2PE Solution Assessment

SecureTrust™ is a division of Trustwave Holdings, Inc.

SERVICE DESCRIPTION

SecureTrust's Point to Point Encryption (P2PE) Solution Assessment (the "**Service**") is designed to identify gaps and prioritize areas that may require remediation to achieve compliance with the Payment Card Industry Point-to-Point Encryption (PCI P2PE) standard set out by the PCI Security Standards Council (SSC) (the "**PCI P2PE standard**"). The Service provides an analysis of PCI P2PE security operations and safeguards.

The Service involves various policies, procedures and practices that will be evaluated by SecureTrust through documentation review, interviews, facilities inspection, controls assessment, and examination of current security architecture.

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 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 as well as 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 Solution 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 report detailing the results of the Service.

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 solution.

Phase I: Information Gathering

SecureTrust and Client will work to gather and analyze information on the P2PE solution. 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 solution.

SecureTrust will examine applicable documentation and may request from Client a remote demonstration of system capabilities to maximize understanding of the P2PE solution functionality, data handling processes, and design parameters, before conducting the review and testing phase of the Service.

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

- Collection of applicable vendor release agreements;
- Secure management of equipment used to encrypt account data;
- Determination of use of third-party support for the solution;
- Review of solution management processes;
- Collection and review of applicable documentation;
- Primary Account Number (PAN) and Sensitive Authentication Data (SAD) protection;
- Point of Interaction (POI) device life cycle, including deployment, maintenance and decommissioning processes;
- Secure device management processes;
- P2PE instruction manual review;
- Decryption environment processes; and
- Review of documented cryptographic operations and methodologies.

Phase II: Review and Testing

The Service may take place onsite within the Client's facilities. Some aspects of the P2PE Solution Assessment may be carried out remotely. SecureTrust will work with Client to determine the testing requirements for each domain of the PCI P2PE standard.

SecureTrust will examine Client's P2PE solution according to applicable P2PE domain testing requirements. Example testing activities may include:

- Observation of the practical implementation of policies, processes and procedures;

- Examination of system configurations;
- Interviews;
- Physical inspection of facilities and equipment;
- Observation of cryptographic operations and methodologies;
- Performance of payment transactions and forensic examinations; and
- Review of third-party support for Client's solution, including PCI DSS and PCI P2PE compliance of those third parties, if applicable.

In addition to Client's facilities, SecureTrust may need to perform onsite testing at any non-P2PE component validated third-party key injection facility (KIF), POI service provider, certificate authority (CA), storage facilities and/or decryption provider used to support the P2PE solution, as applicable.

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 review of Client's P2PE solution, documentation or processes, and procedures.

Phase III: Reporting

SecureTrust will develop a P2PE Report on Validation (P-ROV) documenting observations and recommendations from the Service.

A draft P-ROV will be sent to Client for review. Client will be able to 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 P-ROV and the type of final deliverable to be produced.

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

- If Client's P2PE solution is found compliant with the PCI P2PE standard, and once finalized by SecureTrust's QA group, the final P-ROV together with required supporting documentation will be submitted to the PCI Security Standards Council (SSC) for listing consideration.
- If Client's P2PE Solution 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 within the SecureTrust Portal.
- Interview appropriate organization personnel and collect information from personnel.
- Perform the Service in accordance with the P2PE testing requirements.
- Identify to Client any observations that require remediation.
- Determine the Service results and P2PE solution compliance status.

- Produce either a compliant or a non-compliant P2PE P-ROV, depending on the status of the solution 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.
- Respond to requests from SecureTrust teams when establishing contact and collecting information.
- Accurately 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 uses the requirements and testing procedures of the current version applicable at the time of the Service start date.
    - 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.
    - The Service will begin on the day of the kickoff call. The timeline and termination of the Service 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 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 documentation with direct feedback on any non-compliant observations, and one review of the Client remediated documentation.
    - All PCI services selected in a single SOW or Order Form must be for an identical term.
    - The Service may consist of both onsite and remote assessment activities.
    - 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.
    - 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 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.