SecureTrust
a Trustwave division

Service Description

Point to Point Encryption Component Assessment

Contents

P2PE Component Assessment

SecureTrust™ is a division of Trustwave Holdings, Inc.

SERVICE DESCRIPTION

SecureTrust's Point to Point encryption (P2PE) Component Assessment is a professional services engagement. The P2PE Component Assessment is designed to identify gaps and prioritize areas that may require remediation, in order to achieve compliance with the Payment Card Industry Point-to-Point Encryption (PCI P2PE) standard. The P2PE Component Assessment provides an analysis of PCI P2PE security operations and safeguards.

Overview of the P2PE standard:

Domain 1: Encryption Device and Application Management	The secure management of the PCI-approved POI devices and the resident software.
Domain 2: Application Security	Not applicable to P2PE Component providers.
Domain 3: P2PE Solution Management	Not applicable to P2PE Component providers.
Domain 4: Merchant-managed Solutions	Not applicable to P2PE Component providers.
Domain 5: Decryption Environment	The secure management of the environment that receives encrypted account data and decrypts it.
Domain 6: P2PE Cryptographic Key Operations and Device Management	Establish and administer key management operations for account data encryption POI devices and decryption HSMs.

The P2PE Component Assessment 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.

BASE SERVICE FEATURES

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

DELIVERY AND IMPLEMENTATION

Project Initiation

The SecureTrust GCRS team is assigned to facilitate the successful delivery of the service which includes scheduling and conducting the remote kickoff meeting to define and agree to high-level project plan consisting of milestone dates, key steps, estimates for duration, deliverables, resource requirements and escalation procedures. Client will indicate the P2PE component type to be assessed, as defined by the PCI Security Standards Council (SSC):

- Key injection facility (KIF);
- Certificate or registration authority (CA/RA);
- Encryption management services; or
- Decryption management services.

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

Phase I: Data Gathering

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

SecureTrust will examine applicable documentation and may request a remote demonstration of system capabilities to maximize understanding of the P2PE component’s functionality, data handling processes, and design parameters, before conducting the P2PE Component Review and Testing portion of the assessment.

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 third parties used to support the P2PE component;
- Point of Interaction (POI) device life cycle, including deployment, maintenance and decommissioning processes;
- Secure device management processes;
- Decryption environment processes; and
- Review of documented cryptographic operations and methodologies.

Phase II: P2PE Component Review

The P2PE component review will take place primarily within the Client's facilities. Some aspects of testing may be able to be carried out remotely. SecureTrust will work with Client to determine the testing requirements for each domain of the P2PE standard.

SecureTrust will examine the P2PE component according to all 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;
- Observation of performed processes and procedures;
- Physical inspection of facilities and equipment;
- Observation of cryptographic operations and methodologies;
- Performance of payment transactions and forensic examinations; and
- Review of third parties used to support the P2PE Component, including PCI Data Security Standard (DSS) and PCI P2PE compliance of those third parties, if applicable.

In addition to Client's facilities, SecureTrust will need to perform on-site testing at any non-P2PE Component validated third parties supporting the P2PE component under review.

SecureTrust will work with Client to resolve assessment questions and assist Client in interpreting the requirements and its responses. SecureTrust may request additional P2PE component demonstrations, reviews of applicable code areas, documentation, or data handling processes.

Phase III: Reporting

SecureTrust will develop a P2PE Report on Validation (P-ROV) for submission to 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 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 Solution and Component are found compliant with the P2PE requirements, and once finalized by SecureTrust's QA group, the P-ROV together with required supporting documentation will be submitted to the PCI Security Standards Council (SSC) for listing consideration.

- If the P2PE Solution and Component are found to be non-compliant with the P2PE requirements, SecureTrust will provide Client with a non-compliant 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 in accordance with the P2PE testing procedures.
- Provide Client with information on any findings that requires remediation
- Determine P2PE results and P2PE component compliance status.
- Produce either a compliant or a non-compliant P2PE P-RoV, depending on the status of the component 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:
    - All security and feature updates for SecureTrust Portal software will be included in major version release upgrades.
    - SecureTrust uses the requirements and testing procedures of the current PCI P2PE 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.
- SecureTrust's P2PE Component Assessment uses the requirements and testing procedures of the current P2PE version applicable at the time of the service start date.
- The P2PE validation process consists of both remote and onsite assessment activities.
- The P2PE validation process will begin on the day of the kickoff call. The timeline and termination of the P2PE validation 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 P2PE 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 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.
- 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.
- Lab preparations are the responsibility of Client. Client must provide a lab for the testing that enables testing in accordance with the P2PE requirements. If testing is conducted in the SecureTrust Lab, Client must provide systems that are configured in accordance with the P2PE requirements.
- SecureTrust will perform the service in the English language.
- SecureTrust will not create or modify Client documentation as part of the P2PE Component Assessment.
- SecureTrust will not provide remediation services as part of P2PE Component Assessment.
- 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 submission to the PCI SSC, the fee is levied directly by the PCI SSC.