

Service Description

Point to Point Encryption Gap Assessment

Contents

P2PE Gap Assessment	3
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: P2PE Gap Assessment.....	4
Phase III: Reporting	5
SECURETRUST RESPONSIBILITIES	5
CLIENT RESPONSIBILITIES	5

P2PE Gap Assessment

SecureTrust™ is a division of Trustwave Holdings, Inc.

SERVICE DESCRIPTION

SecureTrust's Point to Point Encryption (P2PE) Gap Assessment (the “**Service**”) helps to identify gaps and prioritize areas that may require remediation to achieve compliance with the Payment Card Industry (PCI) P2PE standard as 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.

SecureTrust evaluates policies, procedures and practices through documentation review, interviews, discussions, facilities inspections, controls analysis, and examination of Client's 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:

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 Gap 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 final 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, component, or application.

Phase I: Information Gathering

SecureTrust and Client will work to gather and analyze information on Client's P2PE solution, component, or 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 of Client's P2PE solution, component, or application.

SecureTrust will examine applicable design documentation to maximize understanding of Client's P2PE solution, component, or application functionality, data handling processes, and design parameters, before conducting the reporting 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 any third-party systems used to support 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;
- Client's P2PE instruction manual review;
- Decryption environment processes; and
- Review of documented cryptographic operations and methodologies.

Phase II: P2PE Gap Assessment

The assessment phase will take place primarily onsite within the Client's facilities. Some aspects of the assessment may be carried out remotely. A SecureTrust security consultant will work with Client to determine the review requirements for each domain of the P2PE standard.

SecureTrust will examine the Client's P2PE solution, component, or application according to applicable PCI P2PE domain review 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; and

- Identification of use of third-party support for Client's P2PE solution, component, application, and a high-level assessment of the PCI DSS and PCI P2PE compliance of those third parties, if applicable.

SecureTrust and Client will work 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, component or application, documentation or processes and procedures.

Phase III: Reporting

SecureTrust will develop the draft report documenting observations and recommendations from Phase II.

The draft report may include identified non-compliant requirements, identified threats, vulnerabilities, or potential vulnerabilities, as well as recommendations to help eliminate or mitigate the risks to Client's systems. Wherever possible, the report includes recommendations of specific changes that may be required to bring Client's P2PE solution, component, or application into compliance with the PCI P2PE standard.

The draft report will be sent to Client for review. Client will be able to comment and suggest changes to the draft report 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 Client with a final report as the final deliverable.

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 gap assessment against the P2PE testing procedures.
- Provide Client with information on any observations that require remediation.
- Determine P2PE Gap Assessment results and solution, component or application compliance status.
- Produce a draft report on the status of the solution, component or application at the time the assessment 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.
 - 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 uses the requirements and testing procedures of the current P2PE version applicable at the time of the Service date.
 - The Service may consist of both remote and onsite assessment activities.
 - 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.
 - The Service does not include in-depth testing or review of system settings, configurations or observation of implemented processes and procedures.
 - The Service does not include visits to third parties used to support the P2PE solution, component or application.
 - 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 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 P2PE Gap Assessment.
 - 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's systems and resources to SecureTrust.