

## **Service Description**

### Point to Point Encryption General Consulting

# Contents

- P2PE General Consulting ..... 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 General Consulting ..... 4
  - Phase III: Reporting ..... 5
  - SECURETRUST RESPONSIBILITIES ..... 5
  - CLIENT RESPONSIBILITIES ..... 5

# P2PE General Consulting

SecureTrust™ is a division of Trustwave Holdings, Inc.

## SERVICE DESCRIPTION

SecureTrust's Point to Point encryption (P2PE) General Consulting (the “**Service**”) is consulting for solution design, application design, policies, procedures and practices employed, or intended for use, by organizations to comply with the Payment Card Industry Point-to-Point Encryption (PCI P2PE) standard as set out by the PCI Security Standards Council (SSC) (the “**PCI P2PE standard**”).

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 scheduling and conducting consulting activities.

**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 review of compensating control.

**P2PE General Consulting** – A SecureTrust P2PE QSA assists Client with general consulting for requirement interpretation, compliance challenges, solution or application design, policies, procedures and any other subject related to the PCI P2PE standard. SecureTrust will provide assistance in analyzing Client's existing or planned PCI P2PE security operations and safeguards through onsite and/or remote consulting, as determined by SecureTrust.

## 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, resource requirements and escalation procedures.

SecureTrust will request initial information 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 examine applicable design documentation to maximize the understanding of Client's P2PE environment's functionality, data handling processes, and design parameters, before delivering the Service.

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

- P2PE environment design;
- Determination of use of third-party support for Client's P2PE solution, component, or application;
- Encryption/Decryption environment design; and
- Key management processes.

### Phase II: P2PE General Consulting

The Service may take place within the Client's facilities, or it may be delivered remotely, as determined by SecureTrust. A P2PE QSA will work with Client to determine the areas of the PCI P2PE standard on which to focus the Service.

SecureTrust will provide Services around areas chosen by Client that relate to the P2PE solution, component or application and will deliver the Service according to the applicable P2PE domains and requirements. SecureTrust and Client will discuss testing requirements and their applicability to Client's solution, component, or application.

Example consulting activities may include:

- Interviews;
- Physical inspection of facilities and equipment;
- Identification of use of third-party for support Client's P2PE solution, component or application; and
- Consulting on specific P2PE requirements.

SecureTrust and Client will work to identify and if possible, 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..

The Service is not intended to focus on any specific controls, unless explicitly requested by Client. The goal of the Service is to assist Client in determining the best course of action for any P2PE focus areas

chosen by Client, and assist Client in determining its ability to undergo a P2PE validation, and to, where possible, identify suggested priority areas for remediation.

### **Phase III: Reporting**

The Service does not include any report deliverable; it is an hourly consulting service offered as consulting at Client's discretion.

SecureTrust will conduct a closeout meeting with client, if desired.

### **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, and resource requirements.
- Schedule and conduct kickoff, periodic status and consulting meetings.
- Interview applicable organization personnel and collect information from personnel.
- Conduct Service activities.
- Provide Client with feedback on any observations identified during the Service that may require remediation.

### **CLIENT RESPONSIBILITIES**

- 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, 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 collection of required 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 uses the requirements and testing procedures of the current PCI P2PE standard applicable at the time of the Service start date.
  - 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.

- 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 PCI Services selected in a single SOW or Order Form must be for an identical term.
- The Service may consist of onsite or 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 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.