SecureTrust
a Trustwave division

Service Description

Payment Card Industry

Token Service Provider Assessment

Contents

Payment Card Industry Token Service Provider Assessment

SecureTrust™ is a division of Trustwave Holdings, Inc.

SERVICE DESCRIPTION

SecureTrust's Payment Card Industry (PCI) Token Service Provider (TSP) Assessment (the "Service") is designed to validate whether identified token data environment (TDE) security operations and controls are compliant with the PCI TSP Security Requirements as set out by the PCI Security Standards Council (the "Standard"). The Service evaluates the design and implementation of an organizations PCI TSP controls and supporting policy, procedures, and practices relevant practices to the 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:

Point to Point Encryption (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 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 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 Standard or the review of a compensating control.

PCI TSP Assessment – The Service validates whether Client's TDE security operations and controls are compliant with the Standard. If Client's TDE is found compliant with Standard, SecureTrust will provide Client with a TSP Report on Compliance (T-ROC) as a declaration of Client's compliance status. If Client's

TDE is found non-compliant with the Standard, SecureTrust will provide a non-compliant T-ROC 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.

Phase I: Information Gathering

SecureTrust and Client will work together to gather and analyze information about Client's TDE. SecureTrust will conduct interviews, as required, with system architects, application developers, database developers, system administrators, quality assurance (QA) or testing personnel and other Client personnel who may provide relevant details.

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

- Description of Client's TDE;
- Description of the components that make up Client's TDE;
- Gather documentation of Client's TDE, including but not limited to diagrams and documentation illustrating Client's TDE internal/external data flows, and internal/external network communication, as applicable;
- List of hardware and software required to run Client's TDE, including any third-party dependencies, as applicable;
- Description of Client's TDE role in the payment lifecycle;
- Functional design specifications showing Client's TDE design and functional implementations;

SecureTrust may request additional information to determine the testing needed to complete the TDE review phase as outlined below.

Phase II: Token Data Environment Review

SecureTrust will conduct documentation reviews, interviews, discussions, evidence reviews, facilities inspections, controls analysis and examination of Client's current security architecture.

The TDE review phase will take place primarily within the Client's facilities. Some aspects of testing may be carried out remotely, solely as determined by SecureTrust.

The TDE review focuses on logical testing of Client's TDE per the requirements outlined in the Standard. The TDE review phase also includes any remaining interviews or documentation reviews, as well as any onsite process observations. SecureTrust will obtain a thorough understanding of how Client's TDE processes data, how it is developed, distributed, configured, and protected from unauthorized access.

SecureTrust will examine Client's execution environment, including review of all tools, functions, software and hardware components, third-party and open-source libraries, requirements, and dependencies, as applicable.

Topics for TDE review include, but are not limited to, the following:

- Token generation, issuing, and mapping processes;

- Assignment of token usage parameters;
- Token lifecycle management;
- Processes to map or re-map tokens, or perform de-tokenization;
- Cryptographic processes to support tokenization functions; and
- Maintenance of underlying token security and related processing controls, such as domain restrictions during transaction processing.

SecureTrust and Client will work together to resolve Client's assessment questions, and SecureTrust will provide Client reasonable assistance in Client's interpretation of the Standard and its responses. SecureTrust may request additional review of Client's TDE, documentation or data handling processes, and procedures.

Phase III: Reporting

SecureTrust will develop a report documenting observations and recommendations from the Service.

The draft report will be sent to Client for review. Client may comment and suggest changes to the draft report 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 report deliverable, as defined below:

- If Client's TDE is found compliant with the Standard, and once finalized by SecureTrust's QA team, the T-ROC will be submitted to Client.
- If Client's TDE is found to be non-compliant with the Standard, SecureTrust will provide Client with a non-compliant T-ROC.

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 in accordance with the PCI TSP testing procedures.
- Provide Client with information on any observations that require remediation.
- Determine Service results and compliance status at the end of the Service.
- Produce either a compliant or a non-compliant T-ROC, depending on the compliance status at the time the Service occurs.
- Deliver to Client a final report documenting all 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 the 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's uses the requirements and testing procedures of the current Standard applicable at the time of the project start date.
    - The Service consists of both remote and onsite assessment activities.
    - The project will begin on the day of the kickoff call where the timeline and end of the project will be determined.
    - Documentation and evidence requested by SecureTrust must be submitted by Client within forty-five (45) days of the start of the project.
        - Client must submit all evidence and complete remediation activities no later than forty-five (45) days prior to the end of the project.
    - 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 includes one onsite assessment.
    - SecureTrust may request evidence from Client's systems and processes as required to assess compliance with any specific requirements. Client agrees to provide all such evidence in a timely manner.
    - 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 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.